IBM Security Trusteer Rapport® for Mitigation

Helps investigate, block, remove, and remediate MitB infected endpoint devices

Highlights

- Enhanced protection to help secure user devices against active financial malware
- Designed to prevent MitB malware infections and remove existing malware to create a safer online banking experience for customers
- Improved investigation capabilities with real-time malware infections and removal notifications

Financial institutions are prime targets for cybercriminal activity with malware being the primary attack tool. Cybercriminals make use of different malware types in order to execute account takeover attacks (ATO), steal credentials and personal information, and initiate fraudulent transactions. Attack tactics, or crime logic, are constantly evolving to become more sophisticated – attempting to better exploit human and system weaknesses.

Man-in-the-browser malware

Web page injection and tampering are examples of common Man-in-the-Browser (MitB) tactics used by cybercriminals in order to trick users into surrendering user credentials and other personal information. This attack is usually achieved via existing vulnerabilities in web browser security allowing fraudsters to modify web pages, modify transaction content or insert additional transactions – all in a completely covert fashion invisible to the end user.

Active MitB malware detection

IBM Security Trusteer Pinpoint™ Detect provides the first line of defense against such attacks. It contains an analytics engine that correlates a wide range of critical fraud indicators—including phishing attacks, malware infections, compromised credentials and advanced evasion methods. Armed with this intelligence, as gathered from 270 million end user endpoints as well as behavioral profiles of end user endpoints, defenses are automatically updated to include the latest defenses.

Additionally, IBM Security Trusteer Pinpoint™ Detect provides your organization with a recommended action in real time along with the detailed reasoning and session details (such as granular device and risk information) behind it. You'll be provided with information about which transactions to allow, which ones to restrict/request step-up-authentication, and which ones require further investigation, and why.

IBM Security Trusteer Pinpoint™ Detect is further enhanced by the investigation capabilities of IBM Security Trusteer Rapport® for Mitigation, an add-on product which is available for purchase for all IBM Security Trusteer Pinpoint™ Detect customers. IBM Security Trusteer Rapport® for Mitigation is based on actionable intelligence that provides organizations with immediate recommendations in the face of malware. It helps detect, remove, and remediate active MitB malware that represents the root cause of most financial fraud.

The information in this document also applies to IBM Security Trusteer Rapport® for Remediation, which is offered as an optional add-on with IBM Security Trusteer Pinpoint Malware Detection.

Rapidly remediating malware infections on end user endpoints

Malware allows cybercriminals to access an end user's computer, account number, and personal information. While malware techniques are constantly evolving to include improved tactics, if an end user's online credentials are stolen via malware, re-credentialing won't necessarily solve the problem if the malware remains on the endpoint.

By integrating IBM Security Trusteer Rapport® for Mitigation, your organization can quickly and easily help end users clean their malware-infected machines. Once malware is suspected on an end user's computer, bank staff simply provide the end user with a link to download IBM Security Trusteer Rapport® for Mitigation, which the end-user can quickly install with one click.

Prevent and remove malware infections

IBM Security Trusteer Rapport® for Mitigation is designed to investigate, remediate, block, and remove dangerous Man-in-the-Browser (MitB) financial malware from infected devices (PC/MACs). It is available on an ad-hoc basis where MitB malware infections have been detected by IBM Security Trusteer Pinpoint™ Detect, and is available only to customers as a tool to investigate and remediate a particular infected device.

Differentiators vs. IBM Security Trusteer Rapport®

IBM Security Trusteer Pinpoint™ Detect customers can purchase IOBM Security Trusteer Rapport® for Mitigation in order to help remediate malware on end user devices. IBM Security Trusteer Rapport® for Mitigation does not provide all of the features of IBM Security Trusteer Rapport® however, it is designed to do the following:

- Actively prevent malware from installing on the endpoint
- Detect and remove active financial malware from infected endpoints
- Protect the particular end user from malicious browser patching
- Warn the particular end user when they attempt to submit credentials into non-secure/risky sites
- Near real-time alerts about immediate threats that require the organization's attention (fraud feeds)

IBM Security Trusteer Rapport® for Mitigation provides a subset of the features available with IBM Security Trusteer Rapport®. For those customers who have purchased IBM Security Trusteer Rapport®, the following additional benefits apply:

- Actively protects the entire end user population of the bank from financial malware capable of stealing online credentials via keylogging, screen capturing, and transaction tampering
- Enforces end user access to the bank's online banking platform via secure HTTPS and validation of the site's SSL certificates
- Shields the browser and protects the entire bank's end user population from host-based threats (BHO/add-ons, DOM, cookies)
- Actively protects entire end users population of the bank against pharming and phishing attacks
- Marketing splash pages designed to peak the entire population of the bank end user's interest in IBM Security Trusteer Rapport®
- Provides access to all reports for IBM Security Trusteer Rapport® in the Financial Trusteer Management Application (TMA).

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven technologies enable organizations to protect their customers, employees and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition.

For more information
To learn more about IBM Security Trusteer Rapport ®, please contact your IBM representative or IBM Business Partner, or visit the following websites: ibm.com/security or ibm.com/software/products/trusteer-rapport

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

Please Recycle
